

Najnowsze wiadomości z Komisji Europejskiej – 30 września 2026

Posted on 1 października, 2026

Najnowsze wiadomości z Komisji Europejskiej – 30 września 2026

Nowy unijny system łączności krytycznej dla służb interwencyjnych

30 września Komisja Europejska zaproponowała **ustanowienie nowego unijnego systemu łączności krytycznej**, aby zapewnić pierwszym europejskim służbom interwencyjnym bezpieczne i odporne kanały komunikacji w sytuacjach kryzysowych. Opierając się na kluczowych komponentach zbudowanych przez europejskie przedsiębiorstwa, nowy system umożliwi płynną i stabilną komunikację w czasie rzeczywistym między wszystkimi służbami interwencyjnymi, przez cały czas i przez wszystkie granice UE, nawet w przypadku niedostępności naziemnych systemów łączności.

Pożary, powodzie, burze, zagrożenia dronami dla infrastruktury krytycznej lub ataki terrorystyczne wymagają skutecznej i dobrze skoordynowanej reakcji ze strony naszej policji, strażaków, służb medycznych i zespołów ochrony ludności. Obecnie ich zdolność do komunikowania się ze sobą jest ograniczona – ich systemy łączności nie są połączone i przestają działać, gdy przekraczają granicę. Oznacza to, że służby ratunkowe często nie mogą komunikować się z innymi, gdy pracują nad ratowaniem ludzi, przywracaniem bezpieczeństwa i bezpieczeństwa publicznego w sytuacjach kryzysowych i nadzwyczajnych.

System łączności krytycznej Unii Europejskiej umożliwi służbom interwencyjnym komunikację transgraniczną oraz udostępnianie zdjęć, nagrań wideo i dźwięku, a także komunikację w sposób szybszy i bezpieczniejszy, zarówno na szczeblu krajowym, jak i w całej Europie. W szczególności:

- Wszystkie państwa członkowskie będą stopniowo przechodzić z wąskopasmowych systemów radiowych na technologię szerokopasmową, **taką jak 5G**, podczas gdy **satelity UE zapewnią** dodatkowe wsparcie w sytuacjach, gdy systemy naziemne są niezdolne do pracy, na przykład podczas

przerw w dostawie prądu.

- EUCCS umożliwi służbom interwencyjnym dzielenie się danymi, materiałami wideo, wiadomościami i geolokalizacją w **czasie rzeczywistym** za pośrednictwem jednego bezpiecznego urządzenia.

Poprawi to orientację sytuacyjną i koordynację w przypadku kryzysów lub sytuacji nadzwyczajnych.

Źródło i więcej informacji: [tutaj](#) oraz [tu](#).

Ochrona praw graczy w UE

[Sieć współpracy w zakresie ochrony konsumentów \(CPC\)](#) rozpoczęła 30 września 2026 skoordynowane działania na szczeblu UE w odniesieniu do dziewięciu firm oferujących gry wideo, mające na celu wzmocnienie ochrony praw graczy.

W ramach tych działań sieć CPC podejmuje działania następcze w związku z [kluczowymi zasadami dotyczącymi walut wirtualnych w grze](#), zestawem wytycznych dotyczących unijnego prawa konsumenckiego, które promują przejrzystość i sprawiedliwość w korzystaniu z walut wirtualnych w grze.

Nowe skoordynowane działania mają na celu zapewnienie stosowania następujących zasad:

- Jasne i przejrzyste ceny;
- Nie zmuszać do niechcianych zakupów walutowych;
- Przed zakupem należy podać jasne informacje;
- Poszanowanie prawa do odstąpienia od umowy;
- Uczciwa i zrozumiała terminologia; warunki gry powinny być uczciwe i jasne dla graczy.
- Ochrona konsumentów podatnych na zagrożenia (np. dzieci).

Więcej: [tutaj](#).

Eurobarometr: trzech na czterech pracowników w UE stanęło w obliczu cyberzagrożeń w miejscu pracy

Jak wynika z nowego [badania Eurobarometru](#) opublikowanego przez Komisję Europejską, **trzech na czterech pracowników w Unii Europejskiej spotkało się z podejrzanymi wiadomościami e-mail, wiadomościami lub linkami w pracy**. Wyniki opublikowano wraz z [rozpoczęciem Europejskiego Miesiąca Cyberbezpieczeństwa](#) we wszystkich 27 państwach członkowskich.

Phishing był najczęstszym cyberzagrożeniem w miejscu pracy, a 39% pracowników zgłaszało fałszywe wiadomości lub strony internetowe zaprojektowane w celu kradzieży danych lub uzyskania nieautoryzowanego dostępu. Pracownicy zgłaszali również próby kradzieży danych osobowych (18%) i haseł (16%), ataków złośliwym oprogramowaniem (17%) oraz oszustw generowanych przez sztuczną inteligencję (15%).

Odkrycia wskazują na lukę między świadomością a codzienną praktyką. Podczas gdy 83% stwierdziło, że potencjalne konsekwencje cyberataków są poważne, tylko 48% stwierdziło, że umie rozpoznać fałszywe wideo wygenerowane przez sztuczną inteligencję. Ogólnie rzecz biorąc, tylko 18% stwierdziło, że ich organizacja – o ile im wiadomo – nie doświadczyła żadnego cyberincydentu.

Więcej [tutaj](#).